Catherine Ybarra (SBN 283360)
Tyler J. Bean (*pro hac vice* to be filed)
SIRI & GLIMSTAD LLP
700 S Flower St, Ste 1000,
Los Angeles, CA 90017
Tel: (646) 357-1732
E: cybarra@sirillp.com
E: tbean@sirillp.com

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

ROY YAX, on behalf of himself and all others similarly situated, Plaintiff, v. SERVICEAIDE, INC. Defendant.	Case No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Roy Yax ("Plaintiff"), individually and on behalf of all similarly situated persons, alleges the following against Serviceaide, Inc. ("Serviceaide" or "Defendant") based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by his counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against Serviceaide for its failure to properly secure and safeguard Plaintiff's and other similarly situated persons' personally identifiable information ("PII") and protected health information ("PHI"), name, Social Security number, data of birth, medical record number, patient account number, medical/health information, health insurance

information, prescription/treatment information, clinical information, provider name, provider location, and email/username (the "Private Information"), from criminal hackers.

2. Serviceaide, based in Santa Clara, is a provider of information technology support management services to Catholic Health and other business clients nationwide (hereinafter, the "Clients" or "Defendant's Clients").

3. On or about May 9, 2025, Serviceaide filed official notice of a hacking incident with the U.S. Department of Health and Human Services. Under state and federal law, organizations must report breaches involving PHI within at least sixty (60) days.

4. On or about the same date, Serviceaide also sent out data breach letters (the "Notice") to individuals whose information was compromised as a result of the hacking incident.

5. Based on the Notice sent to Plaintiff and "Class Members" (defined below), "on November 15, 2024, Serviceaide learned that certain information within its Catholic Health Elasticsearch database was inadvertently made publicly available." In response, the company launched an investigation. The Serviceaide investigation revealed that between September 19, 2024 and November 5, 2024, an unauthorized party had access to certain company files containing the Private Information that Serviceaide stored on behalf of its Clients (the "Data Breach"). Yet, Serviceaide waited six months to notify its Clients and the public that they were at risk.

6. As a result of this delayed response, Plaintiff and Class Members had no idea for six months that their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

7. The Private Information compromised in the Data Breach contained highly sensitive patient data, representing a gold mine for data thieves. The data included, but is not

limited to, name, Social Security number, data of birth, medical record number, patient account number, medical/health information, health insurance information, prescription/treatment information, clinical information, provider name, provider location, and email/username and password that Serviceaide collected and maintained on behalf of its Clients' patients.

8. Armed with the Private Information accessed in the Data Breach (and a head start), data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

9. There has been no assurance offered by Serviceaide that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

10. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

11. Plaintiff brings this class action lawsuit to address Serviceaide's inadequate safeguarding of Class Members' Private Information that it collected and maintained on behalf of its Clients, and its failure to provide timely and adequate notice to its Clients and their affected

patients such as Plaintiff and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

12. The potential for improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to Serviceaide, and thus Serviceaide was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

13. Upon information and belief, Serviceaide failed to properly monitor and implement security practices with regard to the computer network and systems that housed the Private Information. Had Serviceaide properly monitored its networks, it would have discovered the Breach sooner.

14. Plaintiff's and Class Members' identities are now at risk because of Serviceaide's negligent conduct as the Private Information that Serviceaide collected and maintained on behalf of its Clients is now in the hands of data thieves and other unauthorized third parties.

15. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

16. Accordingly, Plaintiff, on behalf of himself and the Class, asserts claims for negligence, negligence *per se*, breach of third party beneficiary contract, unjust enrichment, and declaratory judgment. Plaintiff also brings a claim for Violation of California's Unfair Competition Act, Cal. Bus. & Prof. Code §§ 17200, *et seq*.

II. PARTIES

17. Plaintiff Roy Yax is, and at all times mentioned herein was, an individual citizen of the State of New York.

18. Defendant Serviceaide, Inc. is a provider of information technology support management services with its principal place of business at 2445 Augustine Drive, Suite 150, Santa Clara, California, 95054.

III. JURISDICTION AND VENUE

19. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Serviceaide. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

20. This Court has jurisdiction over Serviceaide because Serviceaide operates in and/or is incorporated in this District.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Serviceaide has harmed Class Members residing in this District.

IV. DIVISIONAL ASSIGNMENT

22. This matter is assigned to the San Jose division pursuant to L.R. 3-2(e).

V. FACTUAL ALLEGATIONS

A. Serviceaide's Business and Collection of Plaintiff's and Class Members' Private Information

23. Serviceaide is a provider of information technology support management services. Founded in 2016, Serviceaide offers AI driven solutions, asset management, and other resources to its Clients. Serviceaide maintains locations in the United States, Latin America, Ukraine, and

Asia. Serviceaide employs more than 90 people and generates approximately $15 million in annual revenue.

24. As a condition of receiving management services, Serviceaide requires that its Clients entrust it with highly sensitive personal information belonging to their patients. In the ordinary course of receiving service from Serviceaide's Clients, Plaintiff and Class Members were required to provide their Private Information to Defendant.

25. In its privacy policy, Serviceaide states "we respect the privacy of our customers, business partners, event attendees, job applicants and Site visitors. We are committed to providing a best-in-class experience, while ensuring the privacy and security of your data. The Company is committed to protecting the privacy of individuals who visit the Site and interact with our Services."[1] Serviceaide also states "[w]e have implemented administrative, technical, and physical security controls that are designed to safeguard your Personal Information."[2]

26. Thus, due to the highly sensitive and personal nature of the information Serviceaide acquires and stores with respect to its patients, Serviceaide, upon information and belief, promises to, among other things: keep patients' Private Information private; comply with industry standards related to data security and the maintenance of its patients' Private Information; inform its patients of its legal duties relating to data security and comply with all federal and state laws protecting patients' Private Information; only use and release patients' Private Information for reasons that relate to the services it provides; and provide adequate notice to patients if their Private Information is disclosed without authorization.

[1] See https://www.serviceaide.com/customer-privacy-statement (last visited May 19, 2025).
[2] *Id.*

27. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Serviceaide assumed legal and equitable duties it owed to them and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

28. Plaintiff and Class Members relied on Serviceaide to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

B. The Data Breach and Defendant's Inadequate Notice to Plaintiff and Class Members

29. According to Defendant's Notice, it learned of unauthorized access to its computer systems on November 15, 2024, with such unauthorized access having taken place between September 19, 2024 and November 5, 2024.

30. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including name, Social Security number, data of birth, medical record number, patient account number, medical/health information, health insurance information, prescription/treatment information, clinical information, provider name, provider location, and email/username, relating to its Clients' patients.

31. On or about May 9, 2025, roughly six months after Serviceaide learned that the Class's Private Information was first accessed by cybercriminals, Serviceaide finally began to notify its Clients and Class Members that its investigation determined that their Private Information was impacted.

32. Serviceaide delivered Data Breach Notification Letters to Plaintiff and Class Members, alerting them that their highly sensitive Private Information had been exposed in a "security incident."

33. Omitted from the Notice are crucial details like the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information is protected.

34. Thus, Serviceaide's purported disclosure amounts to no real disclosure at all, as it fails to inform Plaintiff and Class Members of the Data Breach's critical facts with any degree of specificity. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach was and is severely diminished.

35. In addition, the Notice offers no substantive steps to help victims like Plaintiff and Class Members to protect themselves other than providing one year of credit monitoring – an offer that is woefully inadequate considering the lifelong increased risk of fraud and identity theft Plaintiff and Class Members now face as a result of the Data Breach

36. Serviceaide had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

37. Plaintiff and Class Members provided their Private Information to Serviceaide, either directly or as a result of their healthcare relationship with Catholic Health, one of Serviceaide's Clients, with the reasonable expectation and mutual understanding that Serviceaide would comply with its obligations to keep such information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

38. Serviceaide's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

39. Serviceaide knew or should have known that its electronic records would be targeted by cybercriminals.

C. The Healthcare Sector is Particularly Susceptible to Data Breaches

40. Serviceaide was on notice that companies in the healthcare industry are susceptible targets for data breaches.

41. In August 2014, after a cyberattack on Community Health Systems, Inc., the Federal Bureau of Investigation ("FBI") warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PHI)."[3]

42. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[4]

[3] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), *available at* https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited on May 19, 2025).

[4] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n. (Oct. 4, 2019), *available at*: https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited on May 19, 2025).

43. The healthcare sector reported the second largest number of data breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[5] In 2022, the largest growth in compromises occurred in the healthcare sector.[6]

44. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident … came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[7]

45. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[8]

46. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any

[5] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/wp-content/uploads/2019/01/ITRC_2018-EOY-BREACH-REPORT-KEY-FINDINGS.pdf (last visited on May 19, 2025).

[6] Identity Theft Resource Center, *2022 End-of-Year Data Breach Report, available at*: https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited on May 19, 2025).

[7] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), *available at:* https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/ (last visited on May 19, 2025).

[8] *Id.*

given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[9]

47. Moreover, third-party vendors like Serviceaide are an especially common target for hackers. In 2023, approximately 29-percent of all data breaches resulted from a "third-party attack vector," and as much data breach reporting does not specify the attack vector, "the actual percentage of breaches occurring via third parties was probably higher."[10]

48. As a provider of healthcare-related services, Serviceaide knew, or should have known, the importance of safeguarding the Private Information, including PHI, entrusted to it, and of the foreseeable consequences if such data were to be disclosed. Such consequences include the significant costs imposed on Plaintiff and Class Members due to the unauthorized exposure of their Private Information to criminal actors. Nevertheless, Serviceaide failed to take adequate cybersecurity measures to prevent the Data Breach or the foreseeable injuries it caused.

D. Serviceaide Failed to Comply with HIPAA

49. Title II of HIPAA contains what are known as the Administration Simplification provisions. *See* 42 U.S.C. §§ 1301, *et seq*. These provisions require that HHS create rules to streamline the standards for handling PHI similar to the data Defendant left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

[9] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited on May 19, 2025).

[10] *Global Third-Party Cybersecurity Breaches*, SECURITYSCORECARD (2024), *available online at*: https://securityscorecard.com/reports/third-party-cyber-risk/ (last visited on May 19, 2025).

50. Serviceaide's Data Breach resulted from a combination of insufficiencies that indicate Serviceaide failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from Serviceaide's Data Breach that Serviceaide either failed to implement, or inadequately implemented, information security policies or procedures to protect Plaintiff's and Class Members' PHI.

51. Plaintiff's and Class Members' Private Information compromised in the Data Breach included "protected health information" as defined by CFR § 160.103.

52. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

53. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

54. Plaintiff's and Class Members' Private Information included "unsecured protected health information" as defined by 45 CFR § 164.402.

55. Plaintiff's and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

56. Based upon Defendant's Notice to Plaintiff and Class Members, Serviceaide reasonably believes that Plaintiff's and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

57. Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

58. Serviceaide reasonably believes that Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

59. Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

60. Plaintiff's and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

61. Serviceaide reasonably believes that Plaintiff's and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

62. It is reasonable to infer that Plaintiff's and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

63. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered

unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

64. After receiving notice that they were victims of the Data Breach (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiff and Class Members in this case, to believe that future harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

65. In addition, Serviceaide's Data Breach could have been prevented if Serviceaide had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its patients.

66. Serviceaide's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Serviceaide creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

67. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 also required Serviceaide to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***" (emphasis added).

68. Because Serviceaide has failed to comply with HIPAA, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is also necessary to ensure Serviceaide's approach to information security is adequate and appropriate going forward. Serviceaide still maintains the PHI and other highly sensitive PII of its Clients' patients, including Plaintiff and Class Members. Without the supervision of the Court through injunctive relief, Plaintiff's and Class Members' Private Information remains at risk of subsequent data breaches.

E. Serviceaide Failed to Comply with FTC Guidelines

69. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

70. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[11] The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

71. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, and monitor their networks for suspicious activity.

[11] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (October 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited on May 19, 2025).

72. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45 *et seq*. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

73. Such FTC enforcement actions include those against businesses that fail to adequately protect customer data, like Serviceaide here. *See, e.g.*, *In the Matter of LabMD, Inc*., 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

74. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Serviceaide of failing to use reasonable measures to protect Private Information they collect and maintain from consumers. The FTC publications and orders described above also form part of the basis of Serviceaide's duty in this regard.

75. The FTC has also recognized that personal data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The

larger the data set, the greater potential for analysis and profit."[12]

76. As evidenced by the Data Breach, Serviceaide failed to properly implement basic data security practices. Serviceaide's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

77. Serviceaide was at all times fully aware of its obligation to protect the Private Information of its patients yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

F. Serviceaide Failed to Comply with Industry Standards

78. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

79. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security,

[12] FTC Commissioner Pamela Jones Harbour, *Remarks Before FTC Exploring Privacy Roundtable* (Dec. 7, 2009), *transcript available at* https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited on May 19, 2025).

Incident Response Management, and Penetration Testing.[13]

80. The National Institute of Standards and Technology ("NIST") also recommends certain practices to safeguard systems, such as the following:

a. Control who logs on to your network and uses your computers and other devices.

b. Use security software to protect data.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if possible.

f. Have formal policies for safely disposing of electronic files and old devices.

g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

81. Further still, the United States Cybersecurity and Infrastructure Security Agency ("CISA") makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel

[13] *The 18 CIS Critical Security Controls*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/controls/cis-controls-list (last visited on May 19, 2025).

have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[14]

82. Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiff's and Class Members' Private Information, resulting in the Data Breach.

G. Serviceaide Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information

83. In addition to its obligations under federal and state laws, Serviceaide owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Serviceaide owed a

[14] *Shields Up: Guidance for Organizations*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/shields-guidance-organizations (last visited May 19, 2025).

duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members.

84. Serviceaide breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Serviceaide's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect the Private Information in its possession;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of the Private Information in its possession;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to HIPAA and industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

85. Serviceaide negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

86. Had Serviceaide remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

87. Accordingly, Plaintiff's and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiff and Class Members also lost the benefit of the bargain they made with Serviceaide.

H. Plaintiff and Class Members are at a Significantly Increased and Substantial Risk of Fraud and Identity Theft as a Result of the Data Breach.

88. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[15] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

89. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity

[15] *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on May 19, 2025).

thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

90. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

91. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

92. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

93. One such example of how malicious actors may compile Private Information is through the development of "Fullz" packages.

94. Cybercriminals can cross-reference two sources of the Private Information

compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

95. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

96. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[16] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

[16] *See IdentityTheft.gov*, Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited May 19, 2025).

97. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

98. The Identity Theft Resource Center documents the multitude of harms caused by fraudulent use of PII in its 2023 Consumer Impact Report.[17] After interviewing over 14,000 identity crime victims, researchers found that as a result of the criminal misuse of their PII:

- 77-percent experienced financial-related problems;
- 29-percent experienced financial losses exceeding $10,000;
- 40-percent were unable to pay bills;
- 28-percent were turned down for credit or loans;
- 37-percent became indebted;
- 87-percent experienced feelings of anxiety;
- 67-percent experienced difficulty sleeping; and
- 51-percent suffered from panic of anxiety attacks.[18]

[17] *2023 Consumer Impact Report* (Jan. 2024), IDENTITY THEFT RESOURCE CENTER, *available online at*: https://www.idtheftcenter.org/wp-content/uploads/2023/08/ITRC_2023-Consumer-Impact-Report_Final-1.pdf (last visited on May 19, 2025).

[18] *Id* at pp 21-25.

99. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[19]

100. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

101. While credit card information and associated PII can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[20]

102. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

103. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial

[19] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited on May 19, 2025).

[20] *Data Breaches: In the Healthcare Sector,* CENTER FOR INTERNET SECURITY, *available at*: https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited on May 19, 2025).

repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[21]

104. The ramifications of Serviceaide's failure to keep its patients' Private Information secure are long lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

105. Here, not only was sensitive medical information compromised, but Social Security numbers were compromised too. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

106. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[22]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

[21] Michael Ollove, "*The Rise of Medical Identity Theft in Healthcare*," KAISER HEALTH NEWS (Feb. 7, 2014), *available at*: https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited on May 19, 2025).

[22] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE (June 2007), *available at* https://www.gao.gov/assets/gao-07-737.pdf (last visited on May 19, 2025).

107. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

108. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

I. Plaintiff's and Class Members' Damages

Plaintiff Roy Yax's Experience

109. Upon information and belief, Catholic Health, one of Serviceaide's Clients entrusted it with their patients' Private Information, including the Private Information of Plaintiff Yax.

110. On or about May 9, 2025, Plaintiff Yax received the Notice, which told him that his Private Information had been made publicly available during the Data Breach. The Notice informed him that the Private Information stolen included his "name, Social Security number, data of birth, medical record number, patient account number, medical/health information, health insurance information, prescription/treatment information, clinical information, provider name, provider location, and email/username."

111. The Notice offered Plaintiff Yax only one year of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff Yax will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

112. Plaintiff Yax suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring his accounts for fraud.

113. Plaintiff Yax would not have provided his Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard the Private Information in its possession from theft, or that its systems were subject to a data breach.

114. Plaintiff Yax suffered actual injury in the form of having his PII and PHI compromised and/or stolen as a result of the Data Breach.

115. Plaintiff Yax suffered actual injury in the form of damages to and diminution in the value of his personal, health, and financial information – a form of intangible property that Plaintiff Yax entrusted to Defendant for the purpose of receiving healthcare services from Defendant and which was compromised in, and as a result of, the Data Breach.

116. Plaintiff Yax suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Private Information being placed in the hands of criminals.

117. Plaintiff Yax has a continuing interest in ensuring that his Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches. This interest is particularly acute, as Defendant's systems have already been shown to be susceptible to compromise and are subject to further attack so long as Serviceaide fails to undertake the necessary and appropriate security and training measures to the Private Information.

118. As a result of the Data Breach, Plaintiff Yax made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant. Plaintiff Yax has spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

119. As a result of the Data Breach, Plaintiff Yax has suffered anxiety as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using his PII and PHI for purposes of committing cyber and other crimes against him including, but not limited to, fraud and identity theft. Plaintiff Yax is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on his life.

120. Plaintiff Yax also suffered actual injury from having his Private Information compromised as a result of the Data Breach in the form of (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff Yax through his healthcare provider; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

121. As a result of the Data Breach, Plaintiff Yax anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

122. In sum, Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

123. Plaintiff and Class Members permitted their Private Information be entrusted to Defendant in order to receive services from Defendant's Clients.

124. Their Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

125. As a direct and proximate result of Serviceaide's actions and omissions, Plaintiff and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

126. Further, and as set forth above, as a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

127. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

128. Plaintiff and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiff and Class Members.

129. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiff and Class Members.

130. Plaintiff and Class Members also lost the benefit of the bargain they made with Serviceaide's Clients. Plaintiff and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Upon information and belief, Plaintiff alleges that payments made by Serviceaide's Clients to Serviceaide included payment for cybersecurity protection to protect Plaintiff's and Class Members' Private Information, and that those cybersecurity costs were passed on to Plaintiff and Class Members in the form of elevated prices charged by Serviceaide's Clients for their services. Thus, Plaintiff and the Class did not receive what they paid for.

131. Additionally, Plaintiff and Class Members also suffered a loss of value of their PII and PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[23] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[24]

132. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and

[23] *See How Data Brokers Profit from the Data We Create*, THE QUANTUM RECORD, https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/ (last visited on May 19, 2025).

[24] *Frequently Asked Questions*, NIELSEN COMPUTER & MOBILE PANEL, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited on May 19, 2025).

the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiff and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.

133. Finally, Plaintiff and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

134. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Serviceaide, is protected from future breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing highly sensitive personal and health information of its patients is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

135. As a direct and proximate result of Serviceaide's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

VI. CLASS ACTION ALLEGATIONS

136. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

137. Specifically, Plaintiff proposes the following Nationwide definition (collectively referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
> All individuals in the United States who had Private Information impacted as a result of the Data Breach, including all who were sent a notice of the Data Breach.

138. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

139. Plaintiff reserves the right to modify or amend the definitions of the proposed Nationwide Class, as well as add subclasses, if necessary, before the Court determines whether certification is appropriate.

140. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

141. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of 480,000 patients of Serviceaide's Clients whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Serviceaide's records, Serviceaide's Clients' records, Class Members' records, publication notice, self-identification, and other means.

142. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Serviceaide engaged in the conduct alleged herein;

b. Whether Serviceaide's conduct violated the FTCA and HIPAA;

c. When Serviceaide learned of the Data Breach

d. Whether Serviceaide's response to the Data Breach was adequate;

e. Whether Serviceaide unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

f. Whether Serviceaide failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

g. Whether Serviceaide's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Serviceaide's data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Serviceaide owed a duty to Class Members to safeguard their Private Information;

j. Whether Serviceaide breached its duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether Serviceaide had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

m. Whether Serviceaide breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

n. Whether Serviceaide knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiff and Class Members suffered as a result of Serviceaide's misconduct;

p. Whether Serviceaide's conduct was negligent;

q. Whether Serviceaide's conduct was *per se* negligent;

r. Whether Serviceaide was unjustly enriched;

s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

143. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Serviceaide. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

144. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

145. Predominance. Serviceaide has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Serviceaide's conduct affecting Class Members set out above predominate over

any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

146. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Serviceaide. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

147. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Serviceaide has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

148. Finally, all members of the proposed Class are readily ascertainable. Serviceaide has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Serviceaide.

VII. CLAIMS FOR RELIEF

COUNT I

NEGLIGENCE

(On behalf of Plaintiff and the Nationwide Class)

149. Plaintiff restates and realleges all of the allegations stated above as if fully set forth herein.

150. Serviceaide knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

151. Serviceaide's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

152. Serviceaide knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. Serviceaide was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

153. Serviceaide owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. Serviceaide's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect the Private Information in its possession it using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to HIPAA and the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiff and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

154. Serviceaide's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

155. Serviceaide's duty also arose because Defendant was bound by industry standards to protect the confidential Private Information entrusted to it.

156. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and Serviceaide owed them a duty of care to not subject them to an unreasonable risk of harm.

157. Serviceaide, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Serviceaide's possession.

158. Serviceaide, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

159. Serviceaide, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

160. Serviceaide breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

161. Serviceaide acted with reckless disregard for the rights of Plaintiff and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that

Plaintiff and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

162. Serviceaide had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust Serviceaide with their Private Information was predicated on the understanding that Serviceaide would take adequate security precautions. Moreover, only Serviceaide had the ability to protect its systems (and the Private Information that it stored on them) from attack.

163. Serviceaide's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised and exfiltrated, as alleged herein.

164. Serviceaide's breaches of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

165. As a result of Serviceaide's negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

166. Serviceaide also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the Data Breach.

167. As a direct and proximate result of Serviceaide's negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

168. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

169. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

170. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Serviceaide to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II

NEGLIGENCE PER SE

(On behalf of Plaintiff and the Nationwide Class)

171. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

172. Pursuant to Section 5 of the FTCA, Serviceaide had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and Class Members.

173. Pursuant to HIPAA, 42 U.S.C. § 1302(d), *et seq*., Serviceaide had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

174. Specifically, pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

175. Serviceaide breached its duties to Plaintiff and Class Members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

176. Specifically, Serviceaide breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

177. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII and PHI (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Serviceaide's duty in this regard.

178. Serviceaide also violated the FTCA and HIPAA by failing to use reasonable measures to protect the Private Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

179. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Serviceaide's networks, databases, and computers that stored Plaintiff's and Class Members' unencrypted Private Information.

180. Plaintiff and Class Members are within the class of persons that the FTCA and HIPAA are intended to protect and Serviceaide's failure to comply with both constitutes negligence *per se*.

181. Plaintiff's and Class Members' Private Information constitutes personal property that was stolen due to Serviceaide's negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

182. As a direct and proximate result of Serviceaide's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

183. As a direct and proximate result of Serviceaide's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

184. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Serviceaide to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT III

BREACH OF THIRD-PARTY BENEFICIARY CONTRACT

(On behalf of Plaintiff and the Nationwide Class)

185. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

186. Defendant entered into contracts, written or implied, with its Clients to perform services that include, but are not limited to, providing information technology and management services. Upon information and belief, these contracts are virtually identical between and among

Defendant and its Clients around the country whose patients, including Plaintiff and Class Members, were affected by the Data Breach.

187. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the Private Information of Plaintiff and the Class.

188. These contracts were made expressly for the benefit of Plaintiff and the Class, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its Clients. Defendant knew that if it were to breach these contracts with its Clients, its Clients' patients—Plaintiff and Class Members—would be harmed.

189. Defendant breached the contracts it entered into with its Clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiff's Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately detecting the Data Breach and notifying Plaintiff and Class Members thereof.

190. Plaintiff and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

191. Plaintiff and Class Members are also entitled to their costs and attorney's fees incurred in this action.

COUNT IV

UNJUST ENRICHMENT

(On behalf of Plaintiff and the Nationwide Class)

192. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

193. This Count is pleaded in the alternative to Count III above.

194. Plaintiff and Class Members conferred a benefit on Serviceaide by permitting their healthcare provider, Catholic Health, to turn over their Private Information to Defendant. Moreover, upon information and belief, Plaintiff alleges that payments made by Serviceaide's Clients to Serviceaide included payment for cybersecurity protection to protect Plaintiff's and Class Members' Private Information, and that those cybersecurity costs were passed on to Plaintiff and Class Members in the form of elevated prices charged by Serviceaide's Clients for their services. Plaintiff and Class Members did not receive such protection.

195. Upon information and belief, Serviceaide funds its data security measures entirely from its general revenue, including from payments made to it by its Clients on behalf of Plaintiff and Class Members.

196. As such, a portion of the payments made by Plaintiff and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Serviceaide.

197. Serviceaide has retained the benefits of its unlawful conduct, including the amounts of payment received indirectly from Plaintiff and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

198. Serviceaide knew that Plaintiff and Class Members conferred a benefit upon it, which Serviceaide accepted. Serviceaide profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiff's and Class Members' Private Information and prevented the Data Breach.

199. If Plaintiff and Class Members had known that Serviceaide had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

200. Due to Serviceaide's conduct alleged herein, it would be unjust and inequitable under the circumstances for Serviceaide to be permitted to retain the benefit of its wrongful conduct.

201. As a direct and proximate result of Serviceaide's conduct, Plaintiff and Class Members have suffered, and/or are at a continued, imminent risk of suffering, injury that includes but is not limited to the following: (i) the loss of the opportunity to control how their Private Information is used; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Serviceaide's possession and is subject to further unauthorized disclosures so long as Serviceaide fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

202. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Serviceaide and/or an order proportionally disgorging all profits, benefits, and other

compensation obtained by Serviceaide from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

203. Plaintiff and Class Members may not have an adequate remedy at law against Serviceaide, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT V

VIOLATION OF CALIFORNIA UNFAIR COMPETITION ACT

Cal. Bus. & Prof. Code §§17200, et seq.

(On behalf of Plaintiff and the Nationwide Class)

204. Plaintiff restates and realleges the allegations contained in the preceding paragraphs as if fully set forth herein.

205. Serviceaide is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

206. Serviceaide violated Cal. Bus. & Prof. Code §§ 17200, et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

207. Serviceaide' "unfair" acts and practices include:

a. Serviceaide failed to implement and maintain reasonable security measures to protect Plaintiff's and Class Members' Private Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Serviceaide failed to identify foreseeable security risks, remediate identified security risks, and sufficiently improve security following previous cybersecurity incidents, as described herein. This conduct, with little if any utility, is unfair when

weighed against the harm to Plaintiff and Class Members, whose Private Information has been compromised;

c. Serviceaide's failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, California's Consumer Records Act, Cal. Civ. Code § 1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100;

d. Serviceaide's failure to implement and maintain reasonable security measures also resulted in substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not have known of Serviceaide's grossly inadequate security, consumers could not have reasonably avoided the harms that Serviceaide caused; and

e. Serviceaide engaged in unlawful business practices by violating Cal. Civ. Code § 1798.82.

208. Serviceaide has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), the FTC Act, 15 U.S.C. § 45, and California common law.

209. Serviceaide's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Class Members' Private Information;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, and California's Customer Records Act, Cal. Civ. Code § 1798.80, et

seq., and § 1798.81.5, which was a direct and proximate cause of the Data Breach; and

h. Failing to provide the Notice of Data Breach required by Cal. Civ. Code § 1798.82(d)(1).

210. Serviceaide's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Serviceaide's data security and ability to protect the confidentiality of consumers' Private Information.

211. As a direct and proximate result of Serviceaide's unfair, unlawful, and fraudulent acts and practices, Plaintiff and Class Members were injured and suffered monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Serviceaide's services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

212. Serviceaide acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and Class Members' rights.

213. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Serviceaide's unfair, unlawful, and fraudulent business practices or use of their Private Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT VI

DECLARATORY JUDGMENT

(On behalf of Plaintiff and the Nationwide Class)

214. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

215. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal laws and regulations described in this Complaint.

216. Serviceaide owes a duty of care to Plaintiff and Class Members, which required it to adequately secure Plaintiff's and Class Members' Private Information.

217. Serviceaide still possesses Private Information regarding Plaintiff and Class Members.

218. Plaintiff alleges that Serviceaide's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his Private Information and the risk remains that further compromises of his Private Information will occur in the future.

219. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Serviceaide owes a legal duty to secure its Clients' patients' Private Information and to timely notify them of a data breach under the common law, HIPAA, and the FTCA;

b. Serviceaide's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect patient Private Information; and

c. Serviceaide continues to breach this legal duty by failing to employ reasonable measures to secure its Clients' patients' Private Information.

220. This Court should also issue corresponding prospective injunctive relief requiring Serviceaide to employ adequate security protocols consistent with legal and industry standards to protect patient Private Information in its possession, including the following:

a. Order Serviceaide to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Serviceaide must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Serviceaide's systems on a periodic basis, and ordering Serviceaide to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Serviceaide's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its Clients and their patients about the threats they face with regard to the security of their Private Information, as well as the steps they should take to protect themselves.

221. If an injunction is not issued, Plaintiff will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Serviceaide. The risk of another such breach is real, immediate, and substantial. If another breach at Serviceaide occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

222. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Serviceaide if an injunction is issued. Plaintiff will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Serviceaide's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Serviceaide has a pre-existing legal obligation to employ such measures.

223. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at

Serviceaide, thus preventing future injury to Plaintiff, Class Members, and others whose Private Information would be further compromised.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class described above, seeks the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Serviceaide to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring Serviceaide to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

IX. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: May 19, 2025

Respectfully Submitted,

/s/ *Catherine Ybarra*

Catherine Ybarra (SBN 283360)
SIRI & GLIMSTAD LLP
700 S Flower St, Ste 1000,
Los Angeles, CA 90017
Tel: (646) 357-1732
E: cybarra@sirillp.com

Tyler J. Bean (*pro hac vice* to be filed)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (646) 357-1732
E: tbean@sirillp.com